CLAIMS

What is claimed is:

1. A method comprising:

storing a first list of hardware registers;

receiving video data at an application program;

receiving a second list of hardware registers from a device driver;

determining whether the first list of hardware registers matches the second list of hardware registers; and

if so, streaming the video data to a video decoder.

2. The method of claim 1 further comprising precluding the streaming of the video data to the video decoder if the first list of hardware registers does not match the second list of hardware registers.

3. The method of claim 1 further comprising:

initializing the device driver upon startup of a computer system

forwarding the first list of hardware registers from the device driver to a first security module; and

verifying, at the first security module, a digital signature of the device driver prior to storing the first list of hardware registers.

4. The method of claim 3 further comprising encrypting the first list of

hardware registers prior to storing the first list of hardware registers.

5. The method of claim 1 further comprising:

the application program calling an interface upon receiving the video data;

the interface requesting the second list of hardware registers from the device driver; and

mapping the second list of hardware registers to a virtual resource map that is accessible by the application.

6. The method of claim 5 further comprising:

the interface calling a second security module to verify the second list of hardware registers; and

the second security module calling the first security module in order to verify the virtual resource map.

7. The method of claim 6 further comprising verifying, at the second security module, a digital signature of the interface prior to calling the first security module.

8. The method of claim 7 wherein the second security module calls the first security module via a secure link.

9. A computer system comprising:

a player application that receives data content;

a decoder that stores and decodes the data content received at the player, the decoder including hardware registers to store the data content;

a driver, coupled to the decoder, that allocates the hardware registers within for access by the player application; and

a first security module, coupled to the driver, that secures a first list of resources corresponding to the hardware registers to prevent unauthorized access of the data content within the hardware registers.

10. The computer system of claim 9 wherein the first security module verifies the integrity of the driver via digital signatures prior to receiving the first list of resources.

11. The computer system of claim 9 further comprising an interface, coupled to the player application, the driver and the decoder, that decrypts the content the data content prior to the data content being stored in the hardware registers.

12. The computer system of claim 11 wherein the driver verifies the integrity of the interface via digital signatures and public/private key technologies.

13. The computer system of claim 11 further comprising a second security module coupled to the interface and the first security module.

14. The computer system of claim 13 wherein the second security module receives a second list of resources from the interface whenever the player application is to release the data content from the hardware registers.

15. The computer system of claim 14 wherein the second security module retrieves the first list of resources from the first security module and compares the first list of resources to the second list of resources.

16. The computer system of claim 15 wherein the data content is released from the hardware registers if the second list of resources matches the first list of resources.

17. The computer system of claim 13 wherein the connection between the first security module and the second security module is secured by a random number secret key system.

18. An article of manufacture including one or more computer readable media that embody a program of instructions, wherein the program of instructions, when executed by a processing unit, causes the processing unit to:

store a first list of hardware registers;

receive video data at an application program;

receive a second list of hardware registers from a device driver;

determine whether the first list of hardware registers matches the second list of hardware registers; and

if so, stream the video data to a video decoder.

19. The article of manufacture of claim 18 when executed by a processing unit, further causes the processing unit to preclude the streaming of the video

data to the video decoder if the first list of hardware registers does not match the second list of hardware registers.

20. The article of manufacture of claim 18 when executed by a processing unit, further causes the processing unit to:

initialize the device driver upon startup of a computer system

forward the first list of hardware registers from the device driver to a first security module; and

verify, at the first security module, a digital signature of the device driver prior to storing the first list of hardware registers.

21. The article of manufacture of claim 20 when executed by a processing unit, further causes the processing unit to encrypt the first list of hardware registers prior to storing the first list of hardware registers.

22. The article of manufacture of claim 18 when executed by a processing unit, further causes:

the application program to call an interface upon receiving the video data;

the interface to request the second list of hardware registers from the device driver; and

mapping the second list of hardware registers to a virtual resource map that is accessible by the application.

23. The article of manufacture of claim 22 when executed by a processing

unit, further causes:

the interface to call a second security module to verify the second list of hardware registers; and

the second security module to call the first security module in order to verify the virtual resource map.

24. The article of manufacture of claim 23 when executed by a processing unit, further causes verifying, at the second security module, a digital signature of the interface prior to calling the first security module.